Pegasus (spyware)

Pegasus is spyware developed by the Israeli cyber-arms company NSO Group that can be covertly installed on mobile phones (and other devices) running most[1] versions of iOS and Android.[2] Pegasus is able to exploit iOS versions up to 14.7, through a zero-click exploit.[1] As of 2022, Pegasus was capable of reading text messages, tracking calls, collecting passwords, location tracking, accessing the target device's microphone and camera, and harvesting information from apps.[3][4] The spyware is named after Pegasus, the winged horse of Greek mythology. It is a Trojan horse computer virus that can be sent "flying through the air" to infect cell phones.[5]

Pegasus	
Developer(s)	NSO Group
Initial release	August 2016
Operating system	iOS, Android
Type	spyware
Website	nsogroup.com

Operating system	iOS, Android
Type	spyware
Website	nsogroup.com

Pegasus was discovered in August 2016 after a failed installation attempt on the iPhone of a human rights activist led to an investigation revealing details about the spyware, its abilities, as well as the security vulnerabilities it exploited. News of the spyware caused significant media coverage. It was called the "most sophisticated" smartphone attack ever; it was the first time that a malicious remote exploit used jailbreaking to gain unrestricted access to an iPhone.[6]

The spyware has been used for surveillance of anti-regime activists, journalists, and political leaders from several nations around the world.[7] In July 2021, the investigation initiative Pegasus Project, along with an in-depth analysis by human rights group Amnesty International, reported that Pegasus was still being widely used against high-profile targets.[1]

On January 17, 2023, a book about the Pegasus spyware by investigative journalists, Laurent Richards and Sandrine Rigaud, was published.[8][9]

Background

Technical details

Use by country

Background

NSO Group developed its first iteration of Pegasus spyware in 2011.[4] The company states that it provides "authorized governments with technology that helps them combat terror and crime."[6][10] NSO Group has published sections of contracts which require customers to use its products only for criminal and national security investigations and has stated that it has an industry-leading approach to human rights.[11]

Discovery

Pegasus's iOS exploitation was identified in August 2016. Arab human rights defender Ahmed Mansoor received a text message promising "secrets" about torture happening in prisons in the United Arab Emirates by following a link. Mansoor sent the link to Citizen Lab of the University of Toronto, which investigated, with the collaboration of Lookout, finding that if Mansoor had followed the link it would have jailbroken his phone and implanted the spyware into it, in a form of social engineering.[12]

Citizen Lab and Lookout discovered that the link downloaded software to exploit three previously unknown and unpatched zero-day vulnerabilities in iOS.[13][14] According to their analysis, the software can jailbreak an iPhone when a malicious URL is opened. The software installs itself and collects all communications and locations of targeted iPhones. The software can also collect Wi-Fi passwords.[15]

Google

myanmar government use pegas

All News Images Videos Maps Shopping

International State Crime Initiative
http://statecrime.org › spywareinmy...

Western Tech Firms Sold Spyware to Myanmar's Military Junta

NSO Group claimed that this spyware (called “Pegasus”, after which the investigation takes its name), was intended only for crime control and counter-terrorism ...

People also ask

Is Pegasus still being used?

In which country is Pegasus spyware?

Who uses Pegasus software?

What does the Pegasus program do?

Feedback

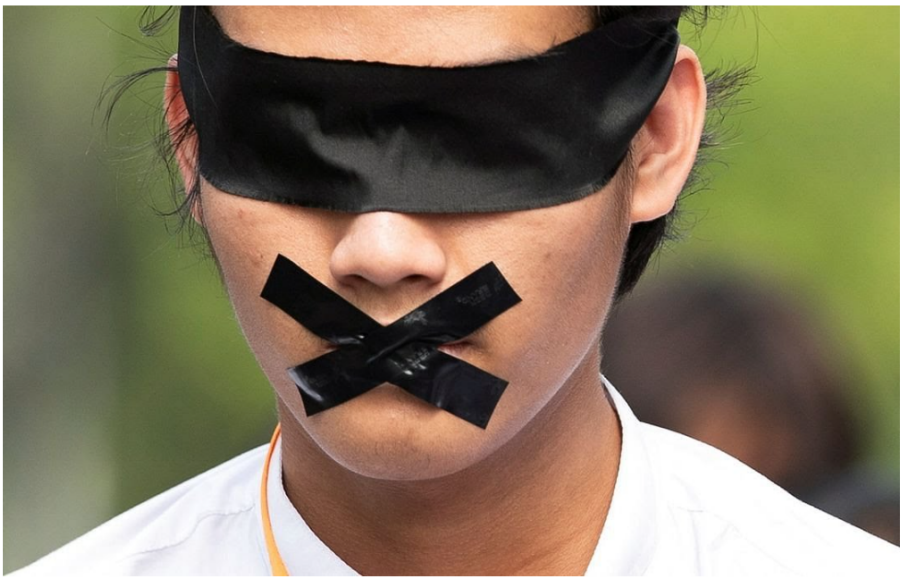
The Daily Star
https://www.thedailystar.net › news

How Myanmar's military moved in on the telecoms sector to spy on citizens

19 May 2021 — Even before the coup, Myanmar's military wielded outsized influence in the democratically elected civilian government led by Suu Kyi.

Published on 11:23 PM, May 19, 2021

How Myanmar's military moved in on the telecoms sector to spy on citizens



A demonstrator protests against the military coup in Yangon, Myanmar, February 19, 2021. REUTERS/Stringer/File Photo

Reuters, Singapore

In the months before the Myanmar military's Feb. 1 coup, the country's telecom and internet service providers were ordered to install intercept spyware that would allow the army to eavesdrop on the communications of citizens, sources with direct knowledge of the plan told Reuters.

The technology gives the military the power to listen in

February 19, 2021. REUTERS/Stringer/File Photo

Reuters, Singapore

In the months before the Myanmar military's Feb. 1 coup, the country's telecom and internet service providers were ordered to install intercept spyware that would allow the army to eavesdrop on the communications of citizens, sources with direct knowledge of the plan told Reuters.

The technology gives the military the power to listen in on calls, view text messages and web traffic including emails, and track the locations of users without the assistance of the telecom and internet firms, the sources said.

The directives are part of a sweeping effort by the army to deploy electronic surveillance systems and exert control over the internet with the aim of keeping tabs on political opponents, squashing protests and cutting off channels for any future dissent, they added.

Decision makers at the civilian Ministry of Transport and Communications that delivered the orders were ex-military officials, according to one industry executive with direct knowledge of the plans and another briefed on the matter.

"They presented it as coming from the civilian government, but we knew the army would have control and were told you could not refuse," the executive with direct knowledge said, adding that officials from the military-controlled Ministry of Home Affairs also sat in on the meetings.

More than a dozen people with knowledge of the intercept spyware used in Myanmar have been

for politicians attempting to form a new civilian government responded to Reuters requests for comment.

Budget documents from 2019 and 2020 for the previous government led by Aung San Suu Kyi that were not disclosed publicly contain details of a planned $4 million in purchases of intercept spyware products and parts as well as sophisticated data extraction and phone hacking technology. The documents were provided by activist group Justice for Myanmar and were independently verified by Reuters.

Reuters was not able to establish to what extent senior non-military people in Suu Kyi's government had been involved in the order to install the intercept.

The idea of a so-called 'lawful intercept' was first floated by Myanmar authorities to the telecommunications sector in late 2019 but pressure to install such technology came only ir
they were w

The intercept plans were flagged publicly by Norway's Telenor in an annual update on its Myann business, which is one of the country's biggest telecom firms with 18 million customers out of a population of 54 million.

Telenor said in the Dec. 3 briefing and statement posted on its websites that it was concerned about Myanmar authorities' plans for a lawful intercept able to "directly access each operator and ISP's systems without case-by-case approval" as Myanmar did not have sufficient laws and regulations to protect customers' rights to privacy and freedom of expression.

In addition to Telenor, the affected companies include three other telecom firms in Myanmar: MPT, a large state-backed operator, Mytel, a venture between Myanmar's army and Viettel which is owned by Vietnam's defence ministry, and Qatar's Ooredoo. MPT

through the appointment of former army officers. That has become total control since the coup.

TRACINGS AND INTERCEPTIONS

According to three sources at firms with knowledge of the surveillance system, not every telecom firm and internet service provider has installed the full intercept spyware. Reuters was not able to establish how broadly it has been installed and deployed.

But military and intelligence agencies are conducting some tracing of SIM cards and interception of calls, two of those sources said. One source said calls being redirected to other numbers and connecting without a dial tone were among the signs of interception.

A legal source with knowledge of cases against people involved in the protests also said there was evidence of monitoring spyware being used to prosecute them. Reuters has not seen any documents supporting the claim.

A senior civil servant who is aiding ousted politicians seeking to form a parallel government also said their group has been warned by people working for the junta but sympathetic to protesters that phone numbers are being traced.

"We have to change SIM cards all the time," the senior civil servant said.

According to Amnesty International's Security Lab and three other tech experts, the intercept products outlined in the government budget documents would enable the bulk collection of phone metadata - data on who users call, when they call and for how long - as well as targeted content interception.

CABLES CUT, ACTIVISTS' PHONES BLOCKED